UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/511,775	05/16/2005	John Heasman	URQU.P-012	6608

57380 7590 02/04/2009

Oppedahl Patent Law Firm LLC
P.O. BOX 4850
FRISCO, CO 80443-4850

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
02/04/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket-oppedahl@oppedahl.com

Office Action Summary	Application No.	Applicant(s)	
	10/511,775	HEASMAN ET AL.	
	Examiner	Art Unit	
	ARAVIND K. MOORTHY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9 and 10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9 and 10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 October 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 13 November 2008.

2. Claims 1-7, 9 and 10 are pending in the application.

3. Claims 1-7, 9 and 10 have been rejected.

4. Claim 8 has been cancelled in a preliminary amendment.

Response to Arguments

5. Applicant's arguments filed 13 November 2008 have been fully considered but they are not persuasive.

On page 1, the applicant argues that Vaidya does not feature the use of "general rules" as featured in current claims 1, 2 and 6. The applicant argues that while Vaidya's use of the term "generic" refers to the target networks associated with a particular (type of) attack, a "general rule" encodes knowledge concerning the impact and/or function of a particular (type of) attack.

The examiner respectfully disagrees. The examiner points out that independent claims 1 and 6 recite "each of the general rules being representative of characteristics associated with plurality of specific instances of intrusion or attempted intrusion". The examiner asserts that the Vaidya reference discloses that the attack signature profiles are descriptive of characteristics of known network security violations. The examiner asserts that the claims do not recite that "generic" refers to the target networks associated with a particular (type of) attack, a "general rule" encodes knowledge concerning the impact and/or function of a particular (type of) attack.

On page 2, the applicant argues with regard to claim 6, the arrangement disclosed in Vaidya does not discloses a means for "automatically generating and storing in a knowledge base new rules".

The examiner respectfully disagrees. Vaidya discloses if no session entry is found in step 102, a new session entry is created in the session cache 44 in step 106. Session data, which includes any matches identified by executing attack signature profile instructions on a data packet, are entered into the new session entry in step 108 and the session entry is entered into the state cache 44 in step 110.

On page 3, the applicant argues that the arrangement disclosed in Vaidya cannot be modified to arrive at the present invention by simply re-implementing it in a logic programming language such as Prolog. The applicant argues that Vaidya's attack signature profiles are categorized into three types: simple, sequential or timer/counter. The applicant argues that the current application is not constrained to this categorization as it considers the impact of potentially dangerous functions rather than detecting known characteristics associated with types of attack.

The examiner respectfully disagrees. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, this enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process. In response to applicant's argument that

the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the impact of potentially dangerous functions) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Objections

6. Claims 1, 6 and 7 are objected to because of the following informalities: misspelling. The word "unauthorized" has been misspelled as "unauthorised". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2 and 6 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya U.S. Patent No. 6,279,113 B1.

As to claim 1, Vaidya discloses an intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network (Vaidya discloses a dynamic network-based signature inspection network Intrusion Detection System (IDS) includes a central data repository 12 and multiple data collectors 10 located on a network such as a Local Area Network 11 (LAN). Although the data collectors 10 are illustrated as stand-alone devices, the function of a data collector can be included on other devices in the

network, such as a server or a router/firewall/switch 20. Multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions [column 5, lines 5-26]). Vaidya discloses the intrusion detection system comprising means for monitoring activity relative to the computer system or network (Vaidya discloses that multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions [column 5, lines 26]). Vaidya disclose means for receiving and storing one or more general rules. Vaidya discloses that each of the general rules being representative of characteristics associated with plurality of specific instances of intrusion or attempted intrusion (Vaidya discloses that in step 56 the communication module 30 of the data repository 12 distributes the signature profiles to the various data collectors 10 throughout the network. Upon receiving a set or sets of attack signature profiles, each data collector 10 stores the set or sets of profiles it receives from the data repository 12 in its signature profile memory 39 [column 6, lines 50-56].Vaidya discloses a method for the operation of the dynamic signature inspection network IDS includes the step 50 of generating attack signature profiles. The attack signature profiles can be generic in that they describe generic network intrusion attempts which are common to most networks [column 6, lines 27-35]). Vaidya discloses matching means for receiving data relating to activity relative to the computer system or network from the monitoring means and for comparing, in a semantic manner, sets of actions forming the activity against the one or more general rules to identify an intrusion or attempted intrusion (Vaidya discloses the attack signature profile is reduced to an expression in step 166 [column 12, lines 1-5]. Vaidya discloses that in step 180 the expression is evaluated to determine in step 182 if the expression matches the packet currently being

analyzed. If the expression does not match, the virtual processor 36 returns a value of false in step 184. If the expression matches the packet, the virtual processor returns a value of true and adds the current time stamp to the application session entry in the state cache 44 in step 186 [column 12, lines 23-29]).

As to claim 2, Vaidya discloses that the one or more general rules forms a knowledge base of the system (Vaidya discloses that in step 52 sets of attack signature profiles are organized according to security requirements of each network object. In step 54, corresponding data that are indicative of which objects corresponds to which sets of attack signature profiles are stored in memory of the data repository 12 [column 6, lines 35-40]). Vaidya discloses that the system comprises means for automatically generating and storing in the knowledge base a new general rule representative of characteristics associated with specific instances of intrusion or attempted intrusion not previously taken into account (Vaidya discloses if no session entry is found in step 102, a new session entry is created in the session cache 44 in step 106. Session data, which includes any matches identified by executing attack signature profile instructions on a data packet, are entered into the new session entry in step 108 and the session entry is entered into the state cache 44 in step 110 [column 9, lines 21-27]).

As to claim 6, Vaidya discloses an intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network (Vaidya discloses a dynamic network-based signature inspection network Intrusion Detection System (IDS) includes a central data repository 12 and multiple data collectors 10 located on a network such as a Local Area Network 11 (LAN). Although the data collectors 10 are illustrated as stand-alone devices, the function of a data collector can be included on other devices in the network,

such as a server or a router/firewall/switch 20. Multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions [column 5, lines 5-26]). Vaidya discloses the intrusion detection system comprising means for monitoring activity relative to the computer system or network (Vaidya discloses that multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions [column 5, lines 26]). Vaidya discloses means for initially receiving and storing a knowledge base comprising one or more general rules. Vaidya discloses that each of the general rules being representative of characteristics associated with a plurality of specific instances of intrusion or attempted intrusion (Vaidya discloses that in step 56 the communication module 30 of the data repository 12 distributes the signature profiles to the various data collectors 10 throughout the network. Upon receiving a set or sets of attack signature profiles, each data collector 10 stores the set or sets of profiles it receives from the data repository 12 in its signature profile memory 39 [column 6, lines 50-56]. Vaidya discloses a method for the operation of the dynamic signature inspection network IDS includes the step 50 of generating attack signature profiles. The attack signature profiles can be generic in that they describe generic network intrusion attempts which are common to most networks [column 6, lines 27-35]). Vaidya discloses means for automatically generating and storing in the knowledge base (after the knowledge base has been initially stored) new general rules representative of characteristics associated with specific instances of intrusion or attempted intrusion not previously taken into account (Vaidya discloses if no session entry is found in step 102, a new session entry is created in the session cache 44 in step 106. Session data, which includes any matches identified by executing attack signature profile instructions on a data packet, are entered

into the new session entry in step 108 and the session entry is entered into the state cache 44 in step 110 [column 9, lines 21-27]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 3-5, 7, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya U.S. Patent No. 6,279,113 B1 in view of "Applications of Inductive Logic Programming" (hereinafter Bratko).

As to claim 3, Vaidya discloses if no session entry is found in step 102, a new session entry is created in the session cache 44 in step 106. Session data, which includes any matches identified by executing attack signature profile instructions on a data packet, are entered into the new session entry in step 108 and the session entry is entered into the state cache 44 in step 110 [column 9, lines 21-27].

Vaidya does not teach that the means for automatically generating and storing a new general rule (i.e. new session entry) comprises inductive logic programming means.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vaidya so that the means for generating and storing a new rule (i.e. updated rules) would have been done by using inductive logic programming.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vaidya by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

As to claims 4, 9 and 10, Vaidya discloses that in step 56 the communication module 30 of the data repository 12 distributes the signature profiles to the various data collectors 10 throughout the network. Upon receiving a set or sets of attack signature profiles, each data collector 10 stores the set or sets of profiles it receives from the data repository 12 in its signature profile memory 39 [column 6, lines 50-56].

Vaidya does not teach that the one or more general rules is or are represented in a logic programming language.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the

positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vaidya so that the rules as taught would have been represented by inductive logic programming.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vaidya by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

As to claim 5, Vaidya discloses that multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions [column 5, lines 26].

Vaidya does not teach that inductive logic programming techniques are applied by the system to an attack an intrusion or attempted intrusion.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vaidya so that the rules of an attack would have been applied by inductive logic programming to derive positive examples.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vaidya by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

As to claim 7, Vaidya discloses an intrusion detection system for detection of intrusion or attempted intrusion by an unauthorized party or entity to a computer system or network (Vaidya discloses a dynamic network-based signature inspection network Intrusion Detection System (IDS) includes a central data repository 12 and multiple data collectors 10 located on a network such as a Local Area Network 11 (LAN). Although the data collectors 10 are illustrated as stand-alone devices, the function of a data collector can be included on other devices in the network, such as a server or a router/firewall/switch 20. Multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions [column 5, lines 5-26]). Vaidya discloses the intrusion detection system comprising means for monitoring activity relative to the computer system or network (Vaidya discloses that multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions [column 5, lines 26]). Vaidya discloses means for

initially receiving and storing in a knowledge base data representative of characteristics associated with one or more specific instances or classes of intrusion or attempted intrusion. (Vaidya discloses that in step 56 the communication module 30 of the data repository 12 distributes the signature profiles to the various data collectors 10 throughout the network. Upon receiving a set or sets of attack signature profiles, each data collector 10 stores the set or sets of profiles it receives from the data repository 12 in its signature profile memory 39 [column 6, lines 50-56]. Vaidya discloses a method for the operation of the dynamic signature inspection network IDS includes the step 50 of generating attack signature profiles. The attack signature profiles can be generic in that they describe generic network intrusion attempts which are common to most networks [column 6, lines 27-35]). Vaidya discloses matching means for receiving data relating to activity relative to the computer system or network from the monitoring means and for comparing sets of actions forming the activity against the stored data to identify an intrusion or attempted intrusion (Vaidya discloses the attack signature profile is reduced to an expression in step 166 [column 12, lines 1-5]. Vaidya discloses that in step 180 the expression is evaluated to determine in step 182 if the expression matches the packet currently being analyzed. If the expression does not match, the virtual processor 36 returns a value of false in step 184. If the expression matches the packet, the virtual processor returns a value of true and adds the current time stamp to the application session entry in the state cache 44 in step 186 [column 12, lines 23-29]).

Vaidya does not teach that the updating means include inductive logic programming means for updating the stored data to take into account characteristics of further instances or

classes of intrusion or attempted intrusion occurring after the knowledge base has been initially received and stored.

Bratko teaches inductive logic programming (ILP). Bratko teaches given background knowledge, expressed as a set of predicate definitions, positive examples and negative examples. Bratko teaches that an ILP system will construct a predicate logic formula such that all the positive examples can be logically derived. Bratko teaches that no negative example can be logically derived [see pages 65-66].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vaidya so that the updating means of the rules would have been done using inductive logic programming.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vaidya by the teaching of Wrobel because one of the main advantages of ILP is ILP's generality of representation for background knowledge. This enables a user to provide, in a more natural way, domain-specific background knowledge to be used in learning. The use of background knowledge enables the user both to develop a suitable problem representation and to introduce problem-specific constraints into the learning process [see page 66].

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431